Assessment of Power Grid Vulnerabilities Accounting for Stochastic Loads and Model Imprecision

Roberto Rocchetta, Edoardo Patelli

Institute for Risk and Uncertainty, Liverpool University
Email: roberto.rocchetta@liverpool.ac.uk
Email: edoardo.patelli@liverpool.ac.uk

Abstract

Vulnerability and robustness are major concerns for future power grids. Malicious attacks and extreme weather conditions have the potential to trigger multiple components outages, cascading failures and large blackouts. Robust contingency identification procedures are necessary to improve power grids resilience and identify critical scenarios. This paper proposes a framework for advanced uncertainty quantification and vulnerability assessment of power grids. The framework allows critical failure scenarios to be identified and overcomes the limitations of current approaches by explicitly considering aleatory and epistemic sources of uncertainty modelled using probability boxes. The different effects of stochastic fluctuation of the power demand, imprecision in power grid parameters and uncertainty in the selection of the vulnerability model have been quantified. Spectral graph metrics for vulnerability are computed using different weights and are compared to power-flow-based cascading indices in ranking $N-1$ line failures and random $N-k$ lines attacks. A rank correlation test is proposed for further comparison of the vulnerability metrics. The IEEE 24 nodes reliability test power network is selected as a representative case study and a detailed discussion of the results and findings is presented.

Keywords: Vulnerability Assessment, Contingency Ranking, Power Grid, Uncertainty, Overload Cascading Failures, Spectral Graph Metrics

1. Introduction

The Power Grid is the world's largest, man-made interconnected structure and plays a critical role in the well-being of society. The working productivity, comfort and safety of local citizens relies on on power grids integrity and even modest power outages can seriously compromise their welfare. Severe blackouts may have a huge social and economic impact and is therefore necessary to develop resilient future power grids, capable of withstanding their occurrences. This requires vulnerability assessments of the electric power supply, the identification of critical scenarios, contingency plans and a high degree of confidence

in the results. It is also necessary to better understand the relationship between power grids operational risks and those associated with a vulnerable topological structure. This will help mitigate the effects of unexpected and hazardous failures, and enhance the overall network robustness and resilience.

The structure and operations of power grids are changing radically [1]-[2]: The growing share of intermittent and uncertain renewable power sources is making grid behaviour less predictable; climate change is predicted to increase the intensity and frequency of extreme weather events with the potential to deeply compromise grid integrity [3]; and as highly meshed (non-radial) distribution grid topology is expected to become more common in the future [4], it is likely to see an increasing structural complexity and interconnection between the power grid components. Due to this scenario of increasing complexity and uncertainty, it is important to assess both the inherent variability in the system and imprecision affecting the network parameters. Topological and operational weaknesses have to be better understood in order to provide superior network designs capable of promptly react to unexpected hazardous situations. One potential method of achieving higher grid resilience is by enhancing existing frameworks for power grid vulnerability assessment and by adopting sophisticated uncertainty quantification techniques.

The robustness of power networks is defined as the degree to which the grid is able to withstand unexpected events without degradation in performance [5]. A closely related concept is the vulnerability, which is generally regarded as the lack of robustness. Vulnerability metrics can be obtained in several ways and, in the literature, overload cascading indices based on power-flow evaluations have been proposed to assess the effect of cascading failure events [6]-[7]. This approach has proven adequate in cases where the cascades are mainly driven by overload line trippings [7]. Alternative approaches have focused on the grid topology by using graph theory to analyse its structure [5]-[8]-[9]-[10]-[11]-[12]-[13]-[14]. The so-called pure topological analysis use unweighted adjacency matrices to calculate vulnerability whilst extended topological approaches enrich the analysis by incorporating electrical engineering information in the weights of the graph. The extended metrics have been introduced based on the idea that pure topological approach may fail in exhaustive captivation of the electric network complexity. Whether or not pure topological approaches and their extended version are capable of fully capture vulnerabilities of power grids is still an open debate [15].

Imprecision is a common problem for power grid models and their parameters, appearing in the calculations due to a number of factors such as, tolerance errors, scarcity of data, inconsistent information, and experts' judgement. This type of uncertainty is generally referred as epistemic or subjective. For example, earlier works dealt with this type of uncertainty using fuzzy power flow analysis [16] or stochastic frameworks for reliability analysis [17]. To the authors' knowledge, topological approaches are generally applied by assuming an exact

knowledge of the network parameters and do not account for uncertainty in the calculations. Authors of Ref. [9] analysed the correlation between vulnerability metrics and power flow models. E. Bompard et al. [10] compared two enhanced metrics (i.e. the extended betweenness and net-ability) by ranking components with respect to the system vulnerability. Recently, Lucas Cuadra et al. [15] reviewed power grid robustness metrics which were computed by adopting complex network theory approaches. G. J. Correa et al. [9]-[18] investigated power network structural vulnerability to single and multiple failures and compared graph-theory approaches against power flow approaches. S. Cvijić and M. Ilić [11] discussed the applicability of graph-theory methods (generally applicable in transportation networks) to power grids. It was showed that some of the physical laws applied to power systems are limiting factors but, when graph-theory methods are applied, the computational cost of analysis is greatly reduced. P. Hines et al. [12] discussed the use of topological measures for power grid vulnerability analysis. Through the analysis of random failures it was argued that topological measures can be useful as general trend indicators of vulnerability, although physical-based models (e.g. power flow models) are believed to be more realistic. S. LaRocca et al. [13] investigated different measures for power grids vulnerability and risk assessment by randomly removing grid components. Similarly, R. Rocchetta and E. Patelli [14] compared graph-theoretic spectral vulnerability metrics to power flow based vulnerability metrics in ranking power grid most critical lines. They showed that load demand uncertainty and tolerance imprecision affect the results of the contingency ranking.

To the authors knowledge, none of the reviewed works analysed the effects of both aleatory and epistemic uncertainty on the computation of graph-theoretic spectral vulnerability metrics. However, it is known that sources of uncertainty will inevitably affect power grids robustness. There are several representative examples which consider these effects in the power grid reliability assessment literature. Few notable approaches include reliability assessments of power grids allocating renewable energy sources [19], increasing interdependency between different networks (e.g. telecommunication network transportation network, etc.) and the inherent variability of the (changing) external environmental conditions [3]. Accounting for relevant sources of uncertainty affecting power grid robustness and vulnerability may help to improve the overall confidence in the results and better identify critical scenarios. Being able to distinguish between the (inherently variable) aleatory component of the uncertainty and the (in principle) reducible epistemic uncertainty can be beneficial for the analysis and for improve confidence in the results. Furthermore, many vulnerability metrics have been proposed in the literature and the results will be inevitably affected by a specific metric selection. It is therefore necessary to assess the level of uncertainty associated to power grid robustness when different metrics are employed for vulnerability analysis.

In this work, drops in performance due to single and multiple line failures are analysed by employing algorithms developed by the authors. A novel weighting

factor based on the line percentage of rating is also introduced and compared to weights applied in the literature. Load demand is inherently variable and the increasing allocation of non programmable renewable energy sources are making its behaviour even more uncertain. Thus, the aleatory and the epistemic uncertainty affecting load demands and network parameters are accounted for and propagated to the vulnerability metrics and respective contributions highlighted. The proposed framework is flexible and can account for renewable energy sources uncertainty. This can be done by proposing a different characterisation of the uncertainty in the load. One of the main contributions of this work is a systematic comparison of the vulnerability based on operational flow-based models and topological approaches (pure and extended). Furthermore, none of the reviewed works compared spectral vulnerability metrics for contingency ranking purposes embedding the methods within advanced uncertainty quantification framework. Thus, similarities and differences of the different metrics are discussed for increasing damage size and accounting for uncertainties due to stochastic loads and line parameters imprecision.

The paper is structured as follows: A concise review on power grid modelling and spectral graph analysis is proposed in Section 2. In Section 3, vulnerability metrics are defined. The uncertainty modelling and contingency analysis are described in Section 4. The developed algorithms and framework are summarised within Section 5. In Section 6 presents the analysis of the IEEE reliability test system. The limitation faced are discussed in Section 7 and in Section 8 conclusions are drawn.

2. Background and Power Grid Modelling

A power network structure can be modelled using weighted or unweighted undirected graphs $\mathcal{G} = \{\mathcal{N}, \mathcal{L}, \mathbf{w}\}$, where $\mathcal{N}$ is the set of network buses (or nodes set), $\mathcal{L}$ is the set of lines connecting the nodes (i.e. links set) and $\mathbf{w}$ is the set of weights associated to the lines [10]-[20]-[21]-[22]. Generally when graph-theory approaches are used, a conservative (pessimistic) hypotesis is made on the network structure, to ease the calculations. Self-loops such as parallel lines are removed from the graph $\mathcal{G}$ and replaced by the equivalent single line model. Different weights define different graph models of the power network, for instance, if $\mathbf{w}$ =1 the model and following analysis will be named purely topological [15], since no electrical quantities are employed. Alternatively, weights can be used to represent specific electrical engineering information. Quantities such as the line susceptance (B_{ij}) or power flow (f_{ij}) have been previously adopted as line weights, see e.g. [8]-[23], where i and j represent the generic nodes. The number of buses and the number of branches in the power network is represented by the cardinality of the node set $N_b = |\mathcal{N}|$ and the cardinality of the line set $N_L = |\mathcal{L}|$, respectively. To simplify the notations the line subscript $(ij) \in \mathcal{L}$ can be replaced with the subscript l representing the line index.

2.1. Overflow Cascading Vulnerability

A 'cascade' is a sequential succession of dependent events [6]. In power systems cascading analysis a failure sequence (lines tripping) can be defined as load-driven when the thermal expansion results in the line dropping beneath its safety clearance, or load-independent such as in case of a mechanical failure. The metric adopted in this paper focuses on load-driven failures and is used to assess the network vulnerability to overload cascading events. The cascading index (CEI) is is obtained computing the 'immediate' post-contingency power-flow operative state and it is defined as follows [6]:

$$CEI(C_{N-k}) = \sum_{l \in \mathcal{L}} \mathcal{P}(C_l|C_{N-k}) \cdot S_l(C_{N-k}) \tag{1}$$

where $\mathcal{P}(C_l|C_{N-k})$ is the probability of a secondary (post-contingency) trip of the line (l) after the contingency denoted as C_{N-k} occurred. The severity $S_l(C_{N-k})$ is a overload severity function for the line l due to the occurrence of a single trip ($k = 1$) or multiple failures ($k > 1$).

Severity functions can be used to quantify the operational risk due to components failures [3]. The continuous severity function for overload is specifically defined for each circuit (lines and transformers). It measures the extent (severity) of failures in terms of line percentage of rating $PR_l = \frac{f_l}{f_{emerg,l}}$. The quantity $f_{emerg,l}$ is the emergency rating of the line $l \in \mathcal{L}$ and is related to its thermal limit and f_l is the power flow in the line. The expression for the continuous severity due to overload (S_l) of a line l is defined as follows [3]:

$$S_l(C_{N-k}) = d * PR_l(C_{N-k}) + c \quad for \quad PR_l \geq PR_l^{min} \tag{2}$$

where S_l is zero for values of the flow rating less than a safety limit PR_l^{min}=0.9. The deterministic limit for the violation of line l is PR_l=1, the near violation region is 0.9$\leq PR_l <$1, and the value PR_l under 0.9 is regarded as safe, parameters of the severity model are d=10 and c=-9. Continuous severity functions provides non zero values for scenarios close to the performance limits, which reflects the realistic sense that close to failure scenarios have non-zero risk (but deterministically safe). The probability of cascading trip of line l after an initiating contingency C_{N-k} occurs can be expressed as follows [6]:

$$\mathcal{P}(C_l|C_{N-k}) = \frac{f_l(C_{N-k}) - f_{0,l}}{f_{trip,l} - f_{0,l}} \tag{3}$$

where $f_l(C_{N-k})$ is the flow on the line l after the contingency C_{N-k} occurred, $f_{trip,l}$ is the flow leading to a certain trip of the line l (assumed to be 1.25 times its thermal limit [6]) and $f_{0,l}$ is the flow in the line l before contingency C_{N-k}. The rationale underpinning Eq.3 is that higher load levels and larger transients increase the likelihood of the secondary contingency (i.e. cascading) on the line l after an initiating event C_{N-k}. The probability $\mathcal{P}(C_l|C_{N-k})$ is set equal 1 for

each $f_l(C_{N-k}) \geq f_{trip,l}$.

The cascading index has indeed some limitations (i.e. the criteria for post-trip probability calculation is based on expert judgement and pre-contingency trip probabilities are neglected). Nevertheless, the computational time needed for its calculation is very small (i.e. that of a single power flow calculation) and this makes it suitable for advanced frameworks for uncertainty quantification, which are generally computationally very demanding.

2.2. Spectral Graph Analysis for Power Grids

The topology of the graph $\mathcal{G}$ can be fully characterised by its adjacency matrix W. An adjacency matrix is a $N \times N$ symmetric matrix in which the non-null elements represent weights of existing lines connecting different nodes. In general, the weight are associated to some measure of interest or set equal to 1 (i.e. unweighted adjacency matrix). The matrix D is the diagonal matrix which contains information about the degrees of each node and its diagonal elements (d_i) are equal the sum of the weights of the lines connected to the node i. The Laplacian L of the matrix W is simply $L = D - W$ and the elements can computed as follows [23]:

$$[L]_{ij} = \begin{cases} \sum_{j}^{N} w_{ij} & \text{if } i = j \\ w_{ij}, & \text{if } i \neq j, (ij) \in \mathcal{L} \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

where the term $\sum_{j}^{N} w_{ij}$ is the degree (d_i) of the node i.

Spectral graph analysis has been recently used to assess power grids robustness [8] and to tackle islanding problems [23]-[24]. The eigen-proprieties of the adjacency matrix are obtained as follows:

$$\begin{aligned} W &= \Phi_W \Lambda \Phi_W^T \\ \Lambda &= [\lambda_1, .., \lambda_N] \end{aligned} \tag{5}$$

Analogously, the spectrum of the network Laplacian is obtained as follows:

$$\begin{aligned} L &= \Phi_L \Psi \Phi_L^T \\ \Psi &= [\mu_1, .., \mu_N] \end{aligned} \tag{6}$$

where $\Phi = [\Phi_1, .., \Phi_N]$ is the set of eigenvectors, Λ is the set of eigenvalues of the adjacency matrix and Ψ is the set of eigenvalues of the Laplacian, such that $0 = \mu_1 \leq \mu_2 \leq ... \leq \mu_N$. The eigenvalues of L are non-negative and the smallest (μ_1) is equal to 0. The multiplicity of μ_1 is equal to the number of connected components. If the graph is disconnected, $\mu_2 = 0$ and at least two separate grids exist. Further details are going to be discussed in Section 3.

3. Vulnerability Metrics and Spectral Analysis for Power Networks

An $N-k$ contingency is defined as the unexpected simultaneous loss of k components in the network [25] (e.g. lines, generators, transformers). Vulnerability indices can be used to quantify the reliability of power networks by assessing relative changes in performance metrics. The network vulnerability $\mathcal{V}(C_{N-k})$ associated to the contingency (C_{N-k}) can be generally quantified as follows [15]:

$$\mathcal{V}(C_{N-k}) = \frac{|\mathcal{M} - \mathcal{M}(C_{N-k})|}{\mathcal{M}} \tag{7}$$

where $\mathcal{M}(C_{N-k})$ is a vulnerability metric after contingency C_{N-k} and $\mathcal{M}$ is the metric value for the undamaged network.

3.1. Pure and Extended Spectral Vulnerability Metrics

Power network structural vulnerability can be assessed by using pure or extended topological models of the grid. The first uses the unweighted adjacency matrix and lines are regarded as identical [15] whilst the second extends the approach by including electrical parameters to weight to the adjacency matrix. Extended topological approaches often made use of the DC approximation, conveniently used to build the adjacency matrix using the grid susceptance matrix [8]. Active power flows have also been used as an alternative weighting factor [15].

In this work, a new weighting factor based on the line percentage of rating is introduced. The weight is compared to existing weights taken from the literature. Thus, the adjacency matrices will built using 4 different weights for each line l (i.e. 1, B_l, f_l and PR_l). The first 3 weights are selected based on earlier works while the percentage of rating is selected on the idea that by weighting lines using f_l relevant information might be missing. For instance, a line that has a very small f_l (e.g. few MW flowing into the lines), can be nonetheless very close to failure (e.g. high PR_l). It is worth remarking that analysis performed using unweighted adjacency matrix or weighted using susceptances have to be regarded as a static analysis (because weights do not change over time). Conversely, using $w_l = f_l$ or $w_l = PR_l$ the analysis has to be regarded as dynamic because weights change over time [23].

Recently, vulnerability metrics obtained from spectral decomposition of W and L have been used to extract indicators of the grid robustness [3]. The metrics considered are: the spectral radius ($\rho_{\mathcal{G}}$) [26], the algebraic connectivity (μ_2) [8]-[3], the natural connectivity $\overline{\lambda}_{\mathcal{G}}$ [27] and effective graph resistance $R_{\mathcal{G}}$ [8]. The Spectral radius is the largest eigenvalue of W whilst μ_2 is the second smallest eigenvalue of L. The natural connectivity and the effective graph resistance can be computed as follow:

$$\overline{\lambda}_{\mathcal{G}} = \ln\left(\frac{1}{N}\cdot\sum_{1=1}^{N} e^{\lambda_i}\right) \tag{8}$$

Spectral Graph-Theoretic Metrics:		$\overline{\lambda}_{\mathcal{G}}$	$R_{\mathcal{G}}$	$\rho_{\mathcal{G}}$	μ_2
Type:	Static		Dynamic		
Weights:	$w_{ij}=1$	$w_{ij}=B_{ij}$	$w_{ij}=f_{ij}$	$w_{ij}=PR_{ij}$	
Approach:	Topological	Extended topological			

Table 1: The spectral graph metrics considered in this work and the weighting factors. Each weight can be associated to different type of approaches (i.e. extended topological, topological, dynamic and static).

$$R_{\mathcal{G}} = N \cdot \sum_{i}^{N} \frac{1}{\mu_i} \tag{9}$$

where λ_i is the i^{th} eigenvalue of W and μ_i is the i^{th} eigenvalue of the L and the sum is such that null μ_i are neglected. The measure $\rho_{\mathcal{G}}$ can be regarded as an indicator of robustness of networks against dynamic processes (e.g. virus spreading, synchronization processes and phase transition behaviours), high μ_2 indicates a highly connected network (difficult to be partitioned into independent components). The natural connectivity quantifies the redundancy of alternative paths by quantifying the weighted number of closed walks of all lengths. The physical meaning is related to the Helmholtz free energy of a network [28] . Finally, $R_{\mathcal{G}}$ computed using susceptances is the sum of effective resistances R_l between all l, the lower it is the higher the network robustness is. The graph spectral radius, the natural connectivity, the algebraic connectivity and the effective graph resistance are computed using the 4 lines weights and used to assess drops in power grids robustness as summarised within Table 1. The overload cascading index presented in Section 2.1 will be for additional comparison between the metrics.

4. Treatment of Uncertainty

4.1. Uncertainty Characterisation

Given a probability space $(\Omega, \mathcal{F}, \mathcal{P})$, a random variable X is defined as a map $X : \omega \in \Omega \rightarrow X(\omega) \in \mathcal{I}_X \subset \mathbb{R}$, which relates basic events ω in the event space Ω to a value $X(\omega)$ included in the random variable support $\mathcal{I}_X$, subset of the real line. In classical probability theory, the measure $X(\omega)$ is a crisp (precise) value, which is obtained assuming exact knowledge of the underlying probability density function $f_X(x)$ (PDF) and related cumulative probability distribution function $F_X(x)$ (CDF). Generally speaking, uncertainty can be divided in aleatory and epistemic [29]-[30]. The aleatory uncertainty (not reducible) explains stochastic behaviours and randomness in events and variables whilst the epistemic uncertainty is commonly related to lack of knowledge, imprecision and poorly designed models and is in theory reducible. In case of incomplete knowledge and lack of sufficient information on $X(\omega)$, it is advisable to relax

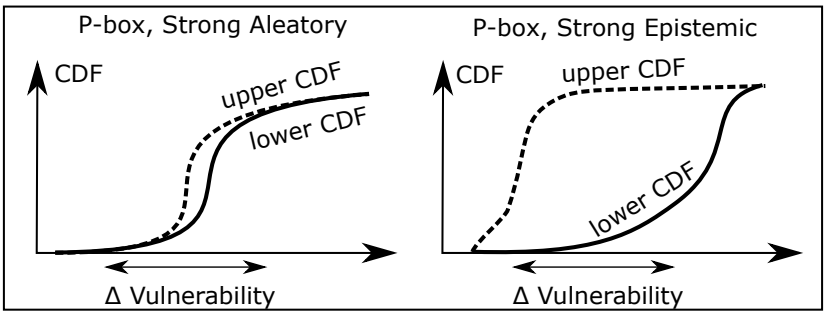

Figure 1: A comparison between two P-boxes. The one on the right hand side has a strong epistemic component.

the assumption on precise probabilistic model. This can be done by employing dedicated theories and approaches (e.g. Evidence theory [31], Imprecise probability [32], Possibility theory [33]).

Probability boxes (P-boxes) are powerful and versatile tools to characterise quantities affected by both aleatory and epistemic uncertainty [32]. P-boxes are strongly connected to Dempster-Shafers theory of evidence [31]-[34]-[35]. Mathematically, a P-box defines upper and lower bounds on CDFs of a random variable, denoted by $\underline{F}_X(x) \leq F_X(x) \leq \overline{F}_X(x)\ \forall x \in \mathcal{I}_X$. The probability boxes can be parametric (or distributional) if the underlying probability distribution family is known (e.g. Gaussian with imprecise mean and variance) or non-parametric (or distribution-free) if the distribution family is not known, e.g. the only information available is on the CDF bounds [29]. Two examples of distribution-free P-boxes are depicted in Fig.1. The distance between the upper and lower CDFs represents the amount of epistemic uncertainty associated to the vulnerability. It can be observed that the P-box on the right hand is strongly affected by epistemic uncertainty. Conversely, the P-box on the left hand side has a stronger aleatory component and the epistemic uncertainty appear to be less relevant.

In this work, the sources of uncertainty investigated are:

1) The aleatory uncertainty associated to load demand variability. The aggregated load connected to a node i ($P_{L,i}$) can be described by a Normal distribution [3] $f(P_{L,i}) = \frac{1}{\sqrt{2\pi}\sigma_i} e^{-\frac{(P_{L,i}-\mu_i)^2}{2\sigma_i^2}}$, where $P_{L,i}$ is the load demand at node i, μ_i is the load mean value and σ_i is the standard deviation at node $i\ \in \mathcal{N}$. The parameter of the distribution can be estimated from historical records of load demand per node.

2) Imprecision in the lines parameters (B_l), attributable to design tolerance modelled as intervals (i.e. epistemic uncertain).

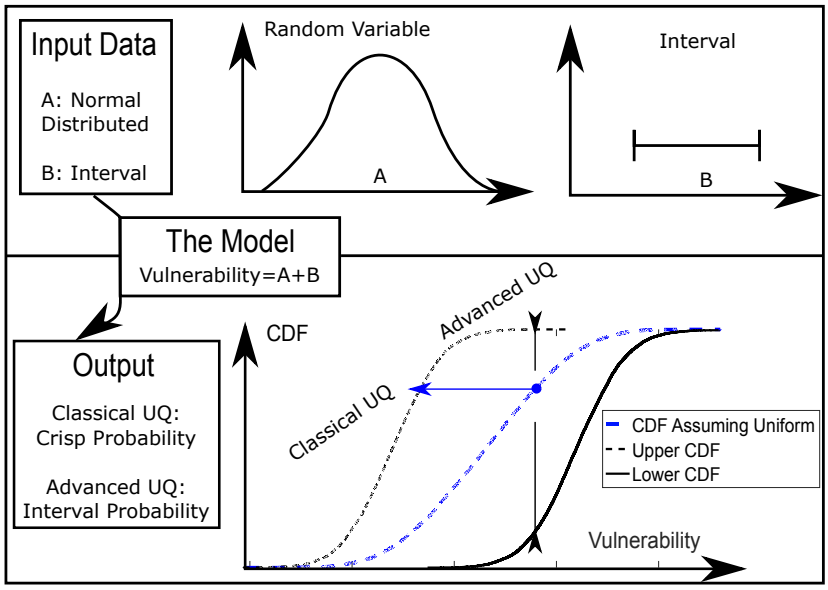

Figure 2: A conceptual comparison between advanced uncertainty quantification and classical uncertainty quantification methods.

3) Uncertainty in the selection of the vulnerability model. Different vulnerability metrics computed using different models (e.g. power-flow model, pure or extended topological models) will be compared and discussed.

Once uncertain inputs are propagated through the computational model, the vulnerability outputs will be characterised by a mixture of aleatory and epistemic uncertainty and described using P-boxes.

4.2. Uncertainty Propagation

Consider a deterministic (computational) vulnerability model $M_{\mathcal{V}}$, is a map from the M-dimensional input space $\mathbf{x}$ to the O-dimensional vulnerability output space $\mathbf{V}$. Formally, it is $M_{\mathcal{V}} : \mathbf{x} \in \mathcal{I}_X \subset \mathbb{R}^M \rightarrow \mathbf{V} = M_{\mathcal{V}}(\mathbf{x}) \in \mathbb{R}^O$, where $\mathbf{x} = (x_1, ..., x_M)$ and $\mathbf{V} = (\mathcal{V}_1, ..., \mathcal{V}_O)$. The computational model can be treated as a black-box of which only the input and output vectors can be processed. If $\mathbf{x}$ is affected by aleatory uncertainty, it will be characterised using appropriate probability distribution function (and corresponding CDF). Once propagated through $M_{\mathcal{V}}$ (e.g. using classical Monte Carlo) the output will result in a well-defined CDF. If $\mathbf{x}$ is affected by epistemic or mixed aleatory-epistemic uncertainty, P-boxes will be suitable for the characterisation. After uncertainty propagation, the outputs will produce bounds on the vulnerability CDFs (i.e. P-boxes).

A simple example which compares a classical probabilistic method to an advanced uncertainty quantification (UQ) method is depicted in Fig.2. A vul-

nerability measure is computed using the mode $M_{\mathcal{V}}$ (sum of A and B), where input A has a well-known aleatory behaviour (e.g. it is distributed as a normal PDF) and the B is a parameter affected by purely epistemic uncertainty (e.g. a tolerance interval). The parameter B does not have a stochastic behaviour, but it is rather imprecisely defined. This is due, for instance, to a limited precision in the available measurements for B. This interval can be narrowed down by providing better instruments for the measurements, i.e. reducing the epistemic uncertainty associated. In order to run a plain MC, uniform distribution is assumed within the interval bounds. Once the probabilistic model is well-defined and uncertainty propagated, the output will have a precise probabilistic description (i.e. a crisp CDF in longdashed line). This might result inappropriate for two main reasons. First, assumptions might be difficult to justify and might produce wrong results. Secondly and perhaps most importantly, the system analysts will be unable to distinguish between the contribution of epistemic uncertainty and aleatory uncertain to the output [32]. Consequently, the analyst will be unable to determine if the output uncertainty is attributable to information deficiency (epistemic problem), that can in theory be reduced, or if is due to randomness and inherent variability (aleatory problem), thus not reducible but just quantifiable. To overcome this limitation, classical probabilistic approaches can be coupled to advanced uncertainty quantification which allows differentiating between epistemic and aleatory uncertainty in the output without introducing assumptions (i.e. uniform random behaviour of a parameter within a tolerance interval) and with weaker or fewer assumptions compared to the classical counterpart. Results are lower and upper bounds on the CDF, in solid and dashed line respectively. The drawback of those methods is the generally higher computational cost [29]-[36] and an imprecise probabilistic description of the output [32], which is the price to pay for slaking the assumptions on the probabilistic model. Nevertheless, generalised probabilistic frameworks provide a valuable perspective on the result and, being non-intrusive, are applicable to any computational model [29].

P-boxes can propagated using different strategies, examples are the double loop Monte Carlo algorithm or the slicing method [37]. Fig.3 presents graphically the two methods. For the slicing method (or focal element propagation) a total of N_s independent samples are directly obtained from the P-box bounds. For each input P-box a so-called 'alpha-cut' α is obtained by sampling from the uniform probability distribution $U(0,1)$. Then, the bounds of the P-boxes are inverted to obtain the input interval as follows:

$$\overline{F}_X(\alpha)^{-1} = \{x|\overline{F}_X(x) = \alpha\} \ \forall \alpha \in [0,1]$$

$$\underline{F}_X(\alpha)^{-1} = \{x|\underline{F}_X(x) = \alpha\} \ \forall \alpha \in [0,1]$$

The combination of the input intervals corresponds to a Parameter cell which is defined by the hyper-rectangle:

$$\mathcal{I}_{X,i} : [\underline{F}_{X1}(\alpha_1)^{-1}, \overline{F}_{X1}(\alpha_1)^{-1}] \times ... \times [\underline{F}_{Xm}(\alpha_m)^{-1}, \overline{F}_{Xm}(\alpha_m)^{-1}]$$

Once the $\mathcal{I}_X$ is sampled, minimum and maximum vulnerabilities are obtained as $\underline{\mathcal{V}}_i = \min_{\mathbf{x}\in\mathcal{I}_{X,i}} M_{\mathcal{V}}(\mathbf{x})$ and $\overline{\mathcal{V}}_i = \max_{\mathbf{x}\in\mathcal{I}_{X,i}} M_{\mathcal{V}}(\mathbf{x})$, respectively. The procedure stops when a total of N_s hyper-rectangles $\mathcal{I}_X$ are sampled and empirical upper and lower CDF bounds computed as:

$$\underline{F}_e(\mathcal{V}) = \frac{1}{N_s}\sum_{i=1}^{Ns} 1_{\mathcal{V}\leq\overline{\mathcal{V}}_i} \qquad \overline{F}_e(\mathcal{V}) = \frac{1}{N_s}\sum_{i=1}^{Ns} 1_{\mathcal{V}\leq\underline{\mathcal{V}}_i}$$

In order to obtain $\overline{\mathcal{V}}_i$ and $\underline{\mathcal{V}}_i$, a variety of methods can be used. For instance, bounds can be approximated by sampling within $\mathcal{I}_X$, using vertex methods [38] or by global optimisation approaches [29]. In this work, a simple and effective (but not efficient) double loop MC [29] is employed. A first loop (outer loop) samples from the epistemic uncertainty space. Each epistemic space realisation correspond a traditional probabilistic uncertainty quantification problem for which only aleatory type of uncertainty has to be accounted. Then, a MC is used in the inner loop to propagate aleatory uncertainty. The result of the inner loop are not to be averaged over the outer loop but only collected and post processed in order to obtain CDF bounds on the quantity of interest. If a monotonic behaviour of the outputs with respect to the imprecise inputs is observed, the epistemic samples can be focused on the vertex of $\mathcal{I}_X$, greatly reducing the computational cost. For further details on the computational strategy, mathematical foundation and, p-box bounds determination, the reader is referred to [29]-[37]-[32]-[34].

4.3. Contingencies and Combinatorial Problem

In some power flow applications, contingency analysis is performed to constrain the network to safe operational states, for instance, by means of Security Constrained Optimal Power Flows. Those states are safe (e.g. thermal constraints are met and no cascading sequence occur) even if one of the contingencies listed is faced by the grid. In general, even if the network has modest size (e.g. small distribution grid), analyse a complete list of all possible failures is infeasible. A comprehensive contingency list will include $\sum_{k=1}^{N} N!/k!(N-k)!$ failures, where k is the number of failed components and N the number of network components. Consider, as example, a very small network of just $N = 50$ components, exhaustive contingency list includes 50 single component failures (i.e. $N-1$ contingencies), 4900 $N-2$, 705600 $N-3$, more than $1.32\cdot10^8$ $N-4$ contingencies and so on. In order to proceed with the calculations, a subset of failures is generally selected from the full set of combinations, the one considered more likely and with higher consequences. Higher order contingencies are often forsaken by assuming a negligible probability of facing those events, too low to be relevant. Nevertheless, targeted malicious attacks, extreme weather induced failures and other common cause failure mechanisms have the potential to increase the likelihood of face severe $N-k$ contingencies[39] and have generally higher consequences for the system. In this paper, the complete set of $N-1$

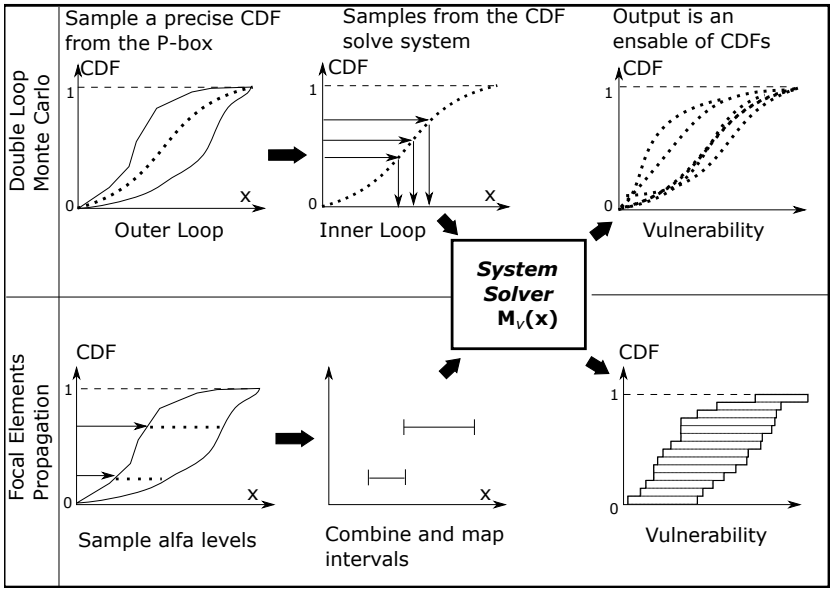

Figure 3: A conceptual comparison of the double loop Monte Carlo (in the top panel) method and the slicing method (in the bottom panel). Figure modified from [37].

single line failure are analysed and the most severe are identified using different vulnerability metrics. Random $N-k$ contingencies are also analysed and for increasing damage size k. The most threatening events will be ranked and the average network vulnerability for increasing k discussed. Relevant sources of uncertainty have been accounted in all the phases of the calculation.

5. The Proposed Framework

Algorithms (designed by the authors) are presented here and will be used to analyse the power grid under $N-1$ and $N-k$ line contingency scenarios. These will be later coupled to advanced, non-intrusive, uncertainty quantification approaches. Algorithm 1 is used for the $N-1$ contingency analysis. First, a power grid case study is loaded (e.g. a MATPOWER '*Case*' [40]) and additional input provided. A pre-contingency power flow (AC or DC) is solved and lines flows f_l and rating PR_l are obtained for the undamaged network. The weights w_l are selected, the undamaged adjacency and Laplacian matrices (W_{und} and L_{und}) obtained and used to compute vulnerability as explained in Sections 2.2 and 3. Single-line failures are evaluated one-at-a-time, either using '*Power-Flow Analysis*' and '*Topological Analysis*' methods.

The '*Power-Flow Analysis*' method works as follows:

1) Removed the line l from the undamaged network structure.

2) Compute post-failure f_l and PR_l using the post-contingency power flow presented in Algorithm 2 which is summarised by steps (3-5).

3) Run the depth-first-search algorithm to find the connected components (cc) in the damaged grid.

4) If the network is fully connected (i.e. $cc = 1$), the power flow is solved, line post-contingency flows obtained and percentage of rating computed.

5) If the network is not fully connected (i.e. $cc > 1$), the islands G_{is} with a single node are removed (the islanding is assumed unsustainable). For the remaining islands G_{is}, a slack bus is selected among the P-V nodes generator nodes) and the post-contingency $f_j(C_l)$ and $PR_j(C_l)$ obtained. If the grid island has no generators, the partition is set as isolated (outage).

6) Compute the overload severity and the cascading probability for all survived lines j and the cascading index $CEI(C_l)$ for the failed line l (i.e. the one removed in step 1).

7) The algorithm steps from 1) to 6) are repeated until all $N-1$ line failures are analysed.

Similarly, the '*Topological Analysis*' method proceeds as follows:

1) Remove the line l from W_{und} and compute the damaged network L.

2) Compute eigen-proprieties ($\Phi_{W_{und}}$, $\Phi_{L_{und}}$, Ψ, Λ).

3) Compute the effective graph resistance, the natural connectivity, the spectral radius and the algebraic connectivity as explained in Section 3.1.

4) Evaluate vulnerability to the analysed contingency $\mathcal{V}(C_l)$ as in Equations 7.

5) Repeat the Algorithm steps 1) to 4) until all the single line failures are analysed.

The method used for the $N-k$ line contingency analysis is summarised in the Algorithm 3. First the network data, the size of the contingency k and the number of contingency scenarios to be analysed N_C are selected. Then, k lines are randomly removed from the undamaged network and the consequence are evaluated using both Algorithm 2 and spectral analysis of the damaged adjacency matrix W. The procedure is repeated until N_C scenarios are analysed and the results are statistical description of the vulnerability of each line (e.g. expectations and CDFs). For instance, the expectation of the vulnerability is computed as $E\left[\mathcal{V}(C_{N-k})\right] = \frac{\sum_{i=1}^{N_C} \mathcal{V}_i(C_{N-k})}{N_C}$.

Main difference between Algorithm 1 and 3 is that the first analyses all the possible single line failures while the second considers random line failures of

Algorithm 1 Vulnerability to $N-1$ Line Contingencies

procedure $N-1$ *Line Contingency*
  Load Power Grid '*Case*'
  Input: Load power demand and line parameters
  Run: pre-contingency AC (or DC) power flow
  Select $w_l \in \{1, B_l, f_l, PR_l\}$ and build W_{und} and L_{und}
  Compute & Save $\Phi_{W_{und}}, \Phi_{L_{und}}, \Psi$, Λ and $\mathcal{M} = \{\rho_{\mathcal{G}}, \mu_2, \overline{\lambda}, R_{\mathcal{G}}\}$

  Power-Flow Analysis
  for each line $l \in \mathcal{L}$ **do**
    Reset undamaged state and remove line l
    Run: Post-Contingency Algorithm 2
    Compute $S_j(C_l)$ and $\mathcal{P}(C_j|C_l)$ for each line in service j.
    Compute $CEI(C_l)$
  end for

  Topological Analysis
  for each line $l \in \mathcal{L}$ **do**
    Set $W = W_{und}$ and $w_l = 0$, build L
    Obtain Φ_W, Φ_L, Ψ and Λ and $\mathcal{M}(C_l) = \{\rho_{\mathcal{G}}, \mu_2, \overline{\lambda}, R_{\mathcal{G}}\}$
    Compute $\mathcal{V}(C_l)$ for each metric
  end for
end procedure

Algorithm 2 Post-Contingency Power Flow

procedure *Post-Contingency Power Flow*
  Search for connected components (cc) (depth-first-search)
  if $cc > 1$ **then**
    Check and remove isolated node
    $\forall$ island:
    Select one slack among the P-V nodes
    Run: AC (or DC) power flows
  end if
  if $cc = 1$ **then**
    Run: AC (or DC) power flows
  end if
end procedure

Algorithm 3 Vulnerability to the $N-k$ Line Contingencies

procedure *Vulnerability to an $N-k$ Line Contingency*
  Input: Load Power Grid '*Case*', set k and N_C
  Run: Pre-contingency AC (or DC) power flow
  Select one $w_l \in \{1, B_l, f_l, PR_l\}$ and build W_{und} and L_{und}
  Compute $\Phi_{W_{und}}$, $\Phi_{L_{und}}$, Ψ, Λ and obtain $\mathcal{M} = \{\rho_{\mathcal{G}}, \mu_2, \overline{\lambda}, R_{\mathcal{G}}\}$
  for $i = 1$ to N_C **do**
    Remove k lines randomly and compute L
    Obtain Φ_W, Φ_L, Ψ, Λ and $\mathcal{M}(C_{N-k}) = \{\rho_{\mathcal{G}}, \mu_2, \overline{\lambda}, R_{\mathcal{G}}\}$
    Compute $\mathcal{V}_i(C_{N-k})$ for each metric
    Run: Post-Contingency Algorithm 2
    Compute $S_l(C_{N-k})$ and $\mathcal{P}(C_l|C_{N-k})$ for each line in service k.
    Compute $CEI_i(C_{N-k})$ and restore undamaged topology
  end for
  Compute CDFs and expectations:
  $F_{CEI_i(C_{N-k})}$, $F_{\mathcal{V}(C_{N-k})}$, $E\left[\mathcal{V}(C_{N-k})\right]$, $E\left[CEI_i(C_{N-k})\right]$
end procedure

order k. The main drawback is that it can result time consuming for large size network. Different networks and weights can be easily selected and compared and both topology-based and flow-based analysis performed in a common flexible computational framework. The Algorithms for $N-1$ contingency analysis is used in combination with non-intrusive uncertainty propagation methods. The effect of aleatory uncertainty (stochastic load demand) and epistemic uncertainty (parameters tolerances) on the vulnerability output of Algorithm 1 are propagated using classical MC and double loop MC methods.

6. A Case Study: IEEE 24 node reliability test system

The selected case study is a modified version of the IEEE 24 nodes reliability test system [41]. The grid is realistic, fairly complex and suitable to test the proposed framework. The modified network counts 24 nodes, 17 loads, 34 lines and 33 generators distributed over 11 nodes. Within the grid, there are 11 P-V nodes (i.e. generator nodes) and 13 P-Q nodes (i.e. load nodes). The original network topology has been modified to substitute parallel lines with equivalent single lines (i.e. the lines l_{19-20}, l_{15-21}, l_{18-21} and l_{20-23}). The modified structure is presented in Fig.4 whilst the design data can be found in Refs.[40]-[41].

6.1. Results: N-1 line failures

The $N-1$ line failures are analysed using the Algorithm 1 and using '*Power-Flow Analysis*' and '*Topological Analysis*' methods as presented in Section 5. The vulnerability results obtained using '*Topological Analysis*' method are displayed in Fig.5. The Y-axis display relative changes in spectral vulnerability metrics due to failure of the line l, i.e. $\mathcal{V}(C_l)$. Each line is identified by an identification number (ID) and displayed on the X-axis. On the right hand side

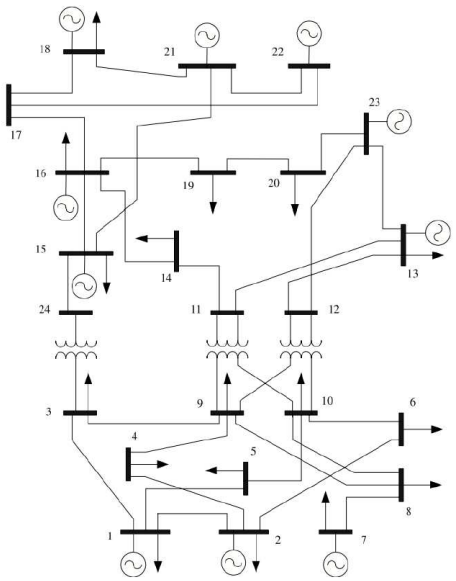

Figure 4: The modified IEEE-RTS 24 nodes layout.

of Fig.5 are presented vulnerability results obtained using μ_2 (the top plot) and $R_{\mathcal{G}}$ (the bottom plot). The relative drops in $\rho_{\mathcal{G}}$ and $\overline{\lambda}$ are presented on the left-hand-side in the bottom and top panels, respectively. Red solid lines are obtained using pure topological analysis ($w_l = 1$), the bars are obtained weighting adjacency with susceptances ($w_l = B_l$), the black dashed lines using the line active flows ($w_l = f_l$) and the green marked lines using percentage of rating ($w_l = PR_l$).

The analysis is performed very efficiently and the 5 most vulnerable lines are ranked in approximatively 0.15 seconds (which is the overall time for all the metrics and weights). The ranking results are presented in Table 2 and pure topological rankings are reported in the first column on the left. The results show similarities and differences in ranks. For instance when algebraic connectivity is employed, the lines l_{7-8} and l_{11-14} are identified as vulnerable, independently from the choice of the lines weights.

The AC power flow and the DC linearised version are used to solve the network and by running the method '*Power-Flow Analysis*' the cascading indices CEI are obtained and line failures ranked. The ranking results for the 5 most vulnerable lines are presented in Table 3. The DC results are quite similar the AC results, although the DC approximation overestimates slightly some of the line flows. This is probably due to the errors introduced by the DC approximation when the network is in contignency state (e.g. for higher system stress, possibly higher losses and larger voltage angles [42]). Furthermore for the selected MATPOWER case, the PV nodes have voltage magnitudes greater than

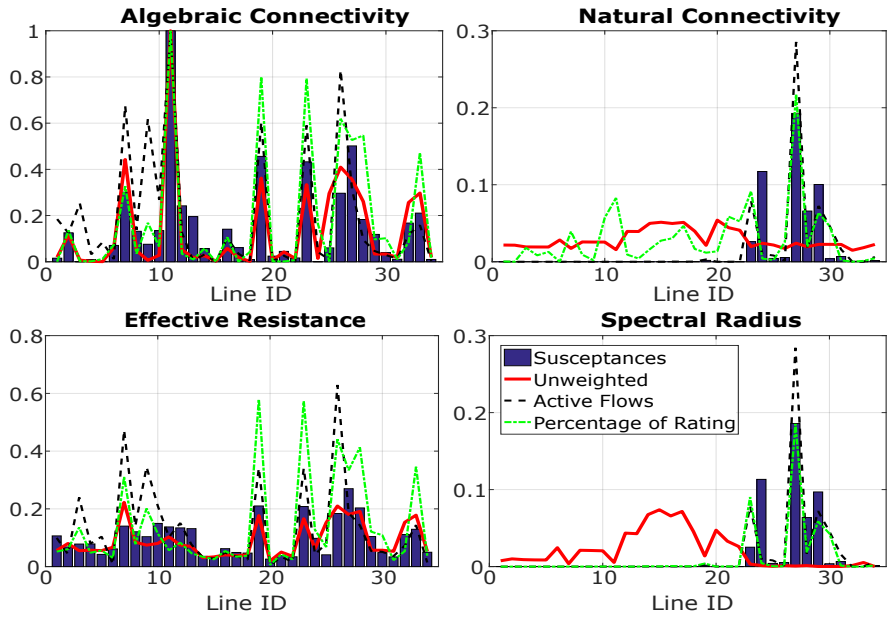

Figure 5: The grid vulnerability to the $N-1$ line failures obtained as relative changes in performance metrics. Comparison between four spectral metrics ($\mu_2, \rho_{\mathcal{G}}, \overline{\lambda}_{\mathcal{G}}, R_{\mathcal{G}}$) and different adjacency matrix weights ($w_l \in \{1, B_l, f_l, PR_l\}$).

	$w_{ij}=1$	$w_{ij}=B_{ij}$	$w_{ij}=f_{ij}$	$w_{ij}=PR_{ij}$
Rank	Algebraic Connectivity μ_2			
1	l_{7-8}	l_{7-8}	l_{7-8}	l_{7-8}
2	l_{3-24}	l_{16-17}	l_{15-24}	l_{11-14}
3	l_{15-24}	l_{11-14}	l_{3-24}	l_{14-16}
4	l_{11-14}	l_{14-16}	l_{5-10}	l_{15-24}
5	l_{16-17}	l_{3-24}	l_{11-14}	l_{16-19}
Rank	Natural Connectivity $\overline{\lambda}_{\mathcal{G}}$			
1	l_{12-13}	l_{16-17}	l_{16-17}	l_{16-17}
2	l_{9-12}	l_{15-16}	l_{14-16}	l_{14-16}
3	l_{10-12}	l_{17-18}	l_{17-18}	l_{7-8}
4	l_{9-11}	l_{16-19}	l_{17-22}	l_{17-18}
5	l_{10-11}	l_{14-16}	l_{16-19}	l_{12-23}
Rank	Spectral Radius $\rho_{\mathcal{G}}$			
1	l_{9-12}	l_{16-17}	l_{16-17}	l_{16-17}
2	l_{10-12}	l_{15-16}	l_{14-16}	l_{14-16}
3	l_{9-11}	l_{17-18}	l_{17-18}	l_{17-18}
4	l_{10-11}	l_{16-19}	l_{17-22}	l_{17-22}
5	l_{12-13}	l_{14-16}	l_{16-19}	l_{16-19}
Rank	Effective Resistance $R_{\mathcal{G}}$			
1	l_{3-24}	l_{16-17}	l_{15-24}	l_{11-14}
2	l_{15-24}	l_{11-14}	l_{3-24}	l_{14-16}
3	l_{16-19}	l_{14-16}	l_{5-10}	l_{15-24}
4	l_{16-17}	l_{16-19}	l_{11-14}	l_{16-19}
5	l_{20-23}	l_{15-24}	l_{14-16}	l_{20-23}

Table 2: The most vulnerable lines for the IEEE 24 nodes reliability test system. The top 5 most vulnerable lines are compared with respect to the 4 spectral metrics obtained using 4 different weighs for the adjacency matrix.

Rank	CEI_{AC}		CEI_{DC}	
1	l_{15-21}	1.00	l_{15-21}	1.33
2	l_{21-22}	0.17	l_{15-24}	0.64
3	l_{15-24}	0.07	l_{3-24}	0.64
4	l_{3-24}	0.07	l_{16-19}	0.22
5	l_{20-23}	0.02	l_{21-22}	0.21

Table 3: The 5 most vulnerable lines from an operational prospective. Comparison between AC and DC results.

1 per-unit, whilst the DC formulation assumes flat voltage profile (i.e. voltage magnitudes set to 1 per-unit). This is likely to affect the calculation and lead to a relevant differences between the DC and AC solutions. Nonetheless, a very good agreement exists between AC and DC rankings (failure of lines l_{15-21}, l_{15-24}, l_{21-22} and l_{3-24} were identified in both lists). It can be concluded that for the analysed network the DC method approximates the AC solutions fairly well also for the aim of contingency ranking. The computational time for the solution for both AC and DC $N-1$ contingency is about 0.9 seconds on a typical desktop PC (8.00 Gb RAM and 2.00 GHz processor). The line l_{15-24} is identified among the 5 most vulnerable by both μ_2 and $R_{\mathcal{G}}$. None of the topological metrics (pure or extended) were able to identify the vulnerability of line l_{15-21}, which scored highest from the overloading cascading perspective. This can be interpreted as a limitation of the topological approaches, which are unable to capture important features in the network operations.

6.1.1. Correlation analysis

An analysis of rank correlations is proposed to assess similarities and differences between the vulnerability metrics. The Spearman's correlation coefficient is a non-parametric measure of rank correlation and it can be used to measure the statistical dependence between metrics. It is sometimes defined as the Pearson correlation coefficient between ranked variables [43]. The matrix of Spearman's rank correlation coefficients is calculated for 2 CEI indices (computed using the AC and DC methods) and for 16 spectral graph metrics (the 4 metrics and 4 weights for each metric). Table 4 presents the correlation results calculated from the ranking of the 10 most vulnerable lines. Figure 6 displays graphically the correlation matrix. It can be observed, as expected, a very high positive correlation between the AC and DC cascading indices (close to 0.8). It can be also observed high/moderate correlations (from 0.6 to 0.9) between the same spectral vulnerability metric but computed with different weights. Algebraic connectivity and effective resistance are also highly correlated, which can be explained as both are computed using the eigenvalues of the Laplacian matrix. Many pairs of vulnerability metrics are weakly correlated (i.e. coefficients <0.3). However, other metrics display a high degree of correlation (i.e. coefficients between 0.6 and 0.9) or a moderate degree of correlation (i.e. coefficients

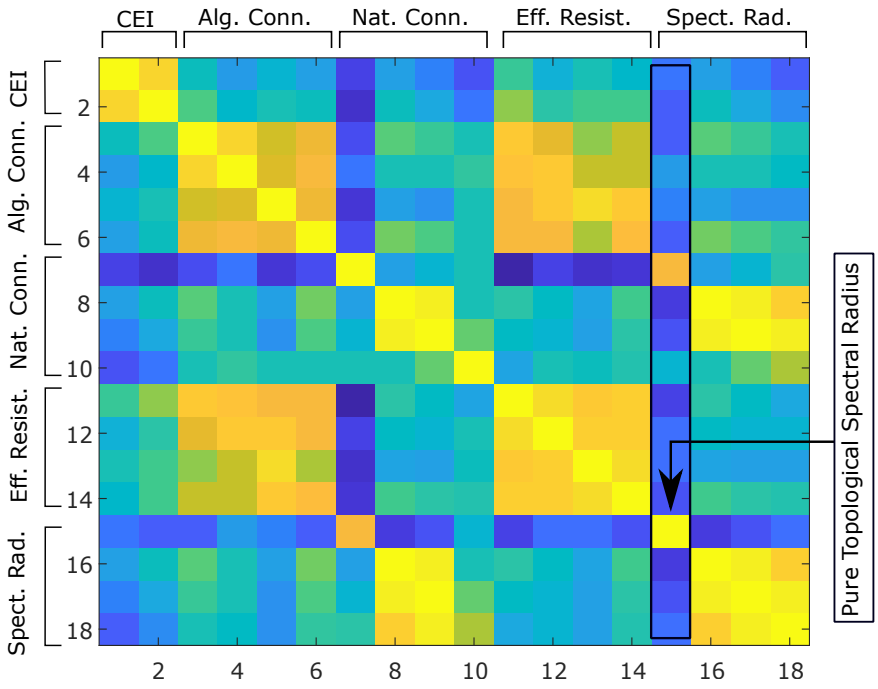

Figure 6: The matrix of Spearman's rank correlation coefficients. It can be observed high correlation between the two CEI indices and between the same topological metric computed using different weights.

between 0.3 and 0.6).

6.1.2. Uncertainty Quantification

The aleatory uncertainty in the power demand is propagated to the cascading index and to the extended topological metrics using the MC method. For each MC run, a random realisation of the load profile is obtained (i.e. a vector containing 17 random loads $P_{L,i}$) and forwarded to the $N-1$ solver (Algorithm 1). The network vulnerability is then evaluated using cascading indices computed with the AC and DC power flow methods. Spectral metrics are computed using 2 different weights for the line (f_{ij} and PR_{ij}). The results for the remaining weights ($w_{ij}=1$ and $w_{ij}=B_{ij}$) are not affect by load variability and thus neglected here. The Monte Carlo method stops when a predefined number of realisations is reached (set to 500).

Figs. 7-8 display the uncertainty quantification results for CEI and the spectral vulnerability metrics, respectively. The red solid lines display the expected vulnerability whilst the blue dashed lines show the expectation plus or minus 2 times the sample standard deviation ($\mathbb{E}[\mathcal{V}(l)] \pm 2\sqrt[2]{\mathbb{V}ar[\mathcal{V}(l)]}$). The red mark-

CEI		μ_2				$\overline{\lambda}_{\mathcal{G}}$				$R_{\mathcal{G}}$				$\rho_{\mathcal{G}}$			
AC	**DC**	**1**	**B**	**f**	**PR**	**1**	**B**	**f**	**PR**	**1**	**B**	**f**	**PR**	**1**	**B**	**f**	**PR**
1.0	0.8	0.1	-0.1	0.1	-0.1	-0.5	-0.1	-0.2	-0.4	0.3	0.0	0.2	0.1	-0.3	-0.1	-0.2	-0.4
0.8	1.0	0.3	0.1	0.2	0.2	-0.6	0.1	0.0	-0.3	0.5	0.2	0.3	0.3	-0.4	0.1	0.0	-0.2
0.1	0.3	1.0	0.8	0.6	0.7	-0.5	0.4	0.3	0.2	0.8	0.6	0.5	0.6	-0.4	0.4	0.3	0.2
-0.1	0.1	0.8	1.0	0.6	0.7	-0.3	0.2	0.2	0.2	0.7	0.8	0.6	0.6	-0.1	0.2	0.2	0.1
0.1	0.2	0.6	0.6	1.0	0.7	-0.6	-0.1	-0.2	0.2	0.7	0.8	0.9	0.8	-0.2	-0.1	-0.2	-0.2
-0.1	0.2	0.7	0.7	0.7	1.0	-0.5	0.4	0.3	0.2	0.7	0.7	0.5	0.7	-0.4	0.4	0.3	0.3
-0.5	-0.6	-0.5	-0.3	-0.6	-0.5	1.0	-0.1	0.1	0.2	-0.7	-0.5	-0.6	-0.6	0.7	-0.1	0.1	0.2
-0.1	0.1	0.4	0.2	-0.1	0.4	-0.1	1.0	0.9	0.2	0.2	0.1	0.0	0.3	-0.5	1.0	0.9	0.8
-0.2	0.0	0.3	0.2	-0.2	0.3	0.1	0.9	1.0	0.4	0.1	0.1	-0.1	0.2	-0.4	0.9	1.0	0.9
-0.4	-0.3	0.2	0.2	0.2	0.2	0.2	0.2	0.4	1.0	0.0	0.2	0.1	0.2	0.1	0.2	0.4	0.5
0.3	0.5	0.8	0.7	0.7	0.7	-0.7	0.2	0.1	0.0	1.0	0.8	0.8	0.8	-0.5	0.2	0.1	0.0
0.0	0.2	0.6	0.8	0.8	0.7	-0.5	0.1	0.1	0.2	0.8	1.0	0.8	0.8	-0.3	0.1	0.1	0.1
0.2	0.3	0.5	0.6	0.9	0.5	-0.6	0.0	-0.1	0.1	0.8	0.8	1.0	0.9	-0.3	0.0	-0.1	-0.1
0.1	0.3	0.6	0.6	0.8	0.7	-0.6	0.3	0.2	0.2	0.8	0.8	0.9	1.0	-0.4	0.3	0.2	0.2
-0.3	-0.4	-0.4	-0.1	-0.2	-0.4	0.7	-0.5	-0.4	0.1	-0.5	-0.3	-0.3	-0.4	1.0	-0.5	-0.4	-0.3
-0.1	0.1	0.4	0.2	-0.1	0.4	-0.1	1.0	0.9	0.2	0.2	0.1	0.0	0.3	-0.5	1.0	0.9	0.8
-0.2	0.0	0.3	0.2	-0.2	0.3	0.1	0.9	1.0	0.4	0.1	0.1	-0.1	0.2	-0.4	0.9	1.0	0.9
-0.4	-0.2	0.2	0.1	-0.2	0.3	0.2	0.8	0.9	0.5	0.0	0.1	-0.1	0.2	-0.3	0.8	0.9	1.0

Table 4: The matrix of the Spearman's rank correlation coefficients. Comparison between the top 10 most vulnerable lines accordingly to the *CEI* indices (AC and DC) and to the 16 spectral graph metrics (4 metrics and 4 weights for each metric).

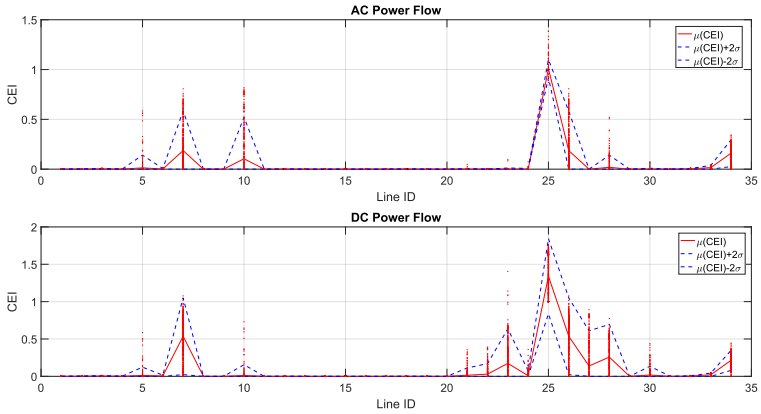

Figure 7: Comparison between AC and DC solver with respect to the variability in the flow-based vulnerability metric. The analysis is performed for the cascading index due to single line failure and random load profiles.

ers are the vulnerability realisations of the MC method (i.e. CEI and $\mathcal{V}$ for each line and for each load demand sample). A 2-sigma rule has been used to robustly rank the 5 most vulnerable lines under uncertainty the results are compared to the deterministic case. Using of a 2-sigma rule means that the rank is based on the upper tail of the vulnerability distribution (i.e. the value selected for the ranking includes 97.73% of the vulnerability realisations if assumed normally distributed). The result significantly changes if compared to the deterministic results presented in Table 3. Table 6 shows the results for the uncertainty quantification on the cascading index applying the AC and the DC solvers. Accordingly to the AC results, the 5 most vulnerable lines are l_{15-21}, l_{15-24}, l_{3-24}, l_{6-10} and l_{21-22}, whilst for the DC result the most vulnerable lines are l_{15-21}, l_{15-24}, l_{3-24}, l_{16-19} and l_{14-16}. The overall computational time needed for the power flow analysis was about 7-8 minutes. On the other hand, the time needed to perform the *Topological Analysis* method was significantly lower, just 68 seconds were needed (i.e. about 17 seconds for each line weight).

The effect of parameter imprecision on the vulnerability result is also assessed. Sources epistemic uncertainty considered are: 10 % imprecision intervals on the 34 lines susceptances, which are attributable to design tolerances. Both the imprecision on B_l and the aleatory uncertainty in the load profile are propagated using a double loop MC approach and without mixing aleatory and epistemic components. Previous analysis suggested that the metrics adopted to assess the vulnerability of the power grid $\mathcal{G}$ vary monotonically with respect the imprecise parameters B_l. Thus, the upper and lower bounds on the CDFs can be efficiently approximated by random search within the vertex boundaries of the hyper-rectangle $\mathcal{I}_X = [0.95B_1, 1.05B_1] \times ... \times [0.95B_{34}, 1.05B_{34}]$. Five-hundred random realisations of B_l from the epistemic space are generated in the outer loop and forwarded to the inner loop where a classical MC samples

	$w_{ij} = f_{ij}$	$w_{ij} = PR_{ij}$	$w_{ij} = f_{ij}$	$w_{ij} = PR_{ij}$
Rank	Expected μ_2 $+2\sigma$		Expected $\overline{\lambda}_{\mathcal{G}}$ $+2\sigma$	
1	l_{7-8}	l_{7-8}	l_{16-17}	l_{16-17}
2	l_{15-24}	l_{11-14}	l_{17-18}	l_{14-16}
3	l_{5-10}	l_{14-16}	l_{14-16}	l_{7-8}
4	l_{1-5}	l_{16-19}	l_{17-22}	l_{17-18}
5	l_{3-24}	l_{20-23}	l_{15-16}	l_{6-10}
Rank	Expected $R_{\mathcal{G}}$ $+2\sigma$		Expected $\rho_{\mathcal{G}}$ $+2\sigma$	
1	l_{15-24}	l_{11-14}	l_{16-17}	l_{16-17}
2	l_{1-5}	l_{14-16}	l_{17-18}	l_{14-16}
3	l_{3-24}	l_{16-19}	l_{14-16}	l_{17-18}
4	l_{5-10}	l_{1-5}	l_{17-22}	l_{17-22}
5	l_{1-3}	l_{20-23}	l_{15-16}	l_{16-19}

	$w_{ij} = f_{ij}$	$w_{ij} = PR_{ij}$	$w_{ij} = f_{ij}$	$w_{ij} = PR_{ij}$
Rank	Expected μ_2 $+2\sigma$		Expected $\overline{\lambda}_{\mathcal{G}}$ $+2\sigma$	
1	1	1	0.36	0.25
2	0.84	0.82	0.10	0.10
3	0.77	0.81	0.09	0.09
4	0.72	0.77	0.06	0.09
5	0.71	0.72	0.03	0.08
Rank	Expected $R_{\mathcal{G}}$ $+2\sigma$		Expected $\rho_{\mathcal{G}}$ $+2\sigma$	
1	0.57	0.53	0.35	0.26
2	0.56	0.51	0.09	0.12
3	0.43	0.49	0.08	0.09
4	0.4	0.45	0.05	0.05
5	0.39	0.44	0.03	0.03

Table 5: The most vulnerable lines for the IEEE 24 nodes reliability test system accordingly to the expectations plus 2σ of topological vulnerability measures.

Rank	Expected CEI_{AC}+2σ		Expected CEI_{DC}+2σ	
1	l_{15-21}	1.05	l_{15-21}	1.84
2	l_{15-24}	0.59	l_{15-24}	1.07
3	l_{3-24}	0.57	l_{3-24}	1.02
4	l_{6-10}	0.51	l_{16-19}	0.69
5	l_{21-22}	0.29	l_{14-16}	0.62

Table 6: The 5 most vulnerable lines accordingly to the CEI expectations plus 2σ. Comparison between AC and DC results.

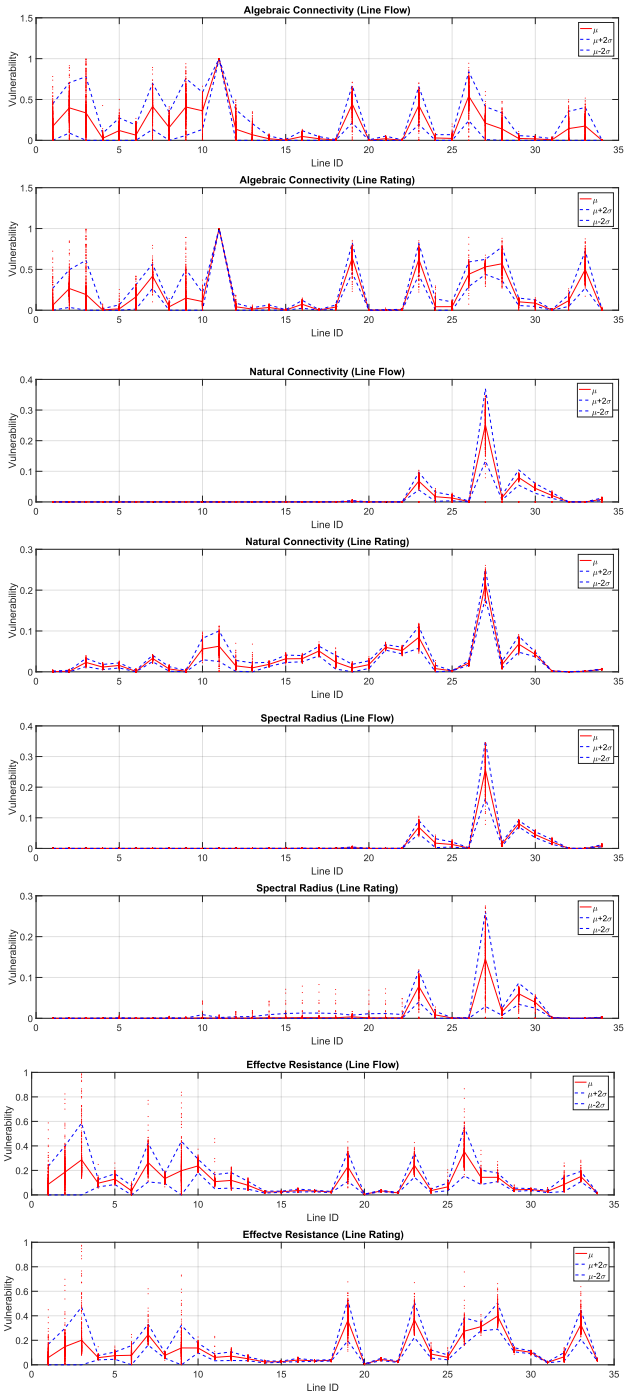

Figure 8: Quantification of the variability of spectral vulnerability metrics due to $N-1$ line failures and random load profiles.

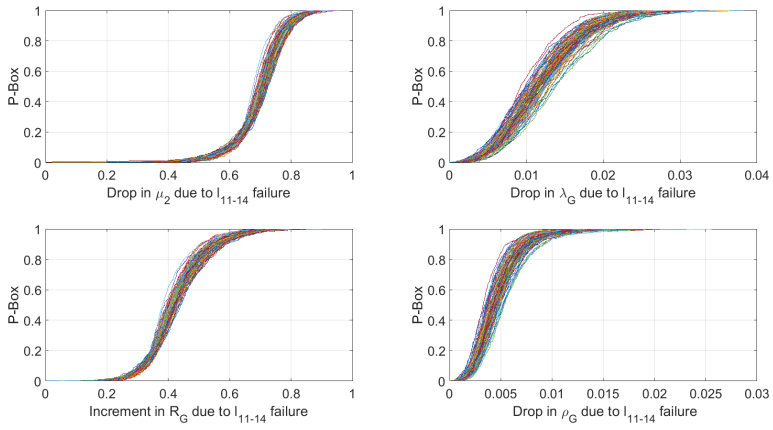

Figure 9: An example of output P-boxes obtained using advanced UQ methods. The vulnerability is greatly affected by aleatory uncertainty, but also epistemic uncertainty plays a role (metrics computed for $w_{ij} = PR_{ij}$).

500 load realisations. The vulnerability is obtained as a P-box and an example is depicted in Fig.9 which presents 4 CDF envelopes (i.e. P-boxes) for the 4 considered metrics and weight $w_{ij} = PR_{ij}$. For sake of synthesis, only vulnerability scores due to failure of l_{11-14} are plotted (other lines produces analogous results). In can be noticed that the aleatory component is dominating the uncertainty associated to the spectral vulnerability metrics. The effect of parameters imprecision has been quantified and it resulted small but observable. Same uncertainty sources have been propagated on the cascading index CEI solving the network using the DC power flow method. The P-boxes of CEI and for two of the most vulnerable lines have been reported in Fig.10. Especially for the failure of the line connecting node 15 to node 21 the CEI precision results highly affected by parameter tolerances. This is an interesting result showing that some failure scenarios are more sensitive to a data deficiency, tolerance imprecision and epistemic uncertainty.

6.2. Results: N-k line failures

Higher order $N - k$ contingencies are analysed using the Algorithm 3 presented in Section 5. The contingency analysis is carried out by increasing damage sizes, i.e. $k = 1, .., 8$. The random number of failures N_C is set equal to 1000 for each damage size k. Fig.11 shows that the average topological vulnerabilities computed weighting adjacency elements by susceptances, which result increasing for increasing k. It is interesting to notice that average drops in spectral radius and the natural connectivity result very similar and that have the lower gradient with respect to the contingency size. Conversely, the mean drop in algebraic connectivity has the higher gradient and for a contingency of

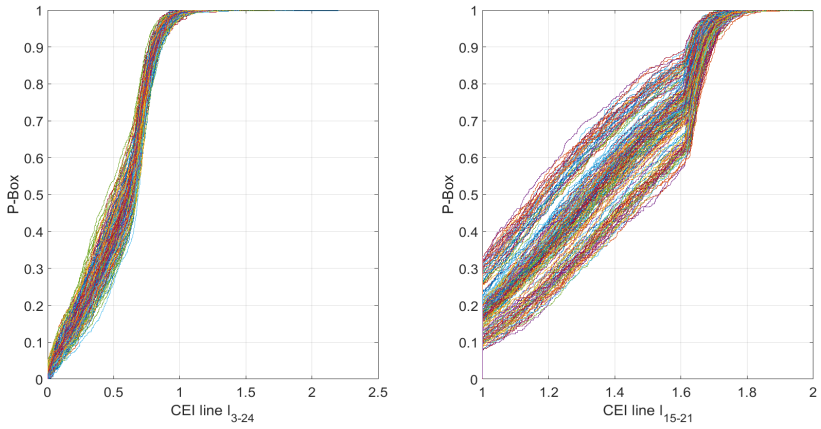

Figure 10: An example of output P-boxes for the CEI indices associated to two vulnerable lines in the system. The index associated to line l_{15-21} is greatly affected by both epistemic and aleatory uncertainty.

type $N-8$, it results close to 1. This indicates that it is highly unlikely to face an $N-8$ failure which keeps the power grid fully connected (i.e. $\mu_2 \neq 0$ for the damaged network). Furthermore, the relative drop in algebraic connectivity will be of little use to analyse higher order contingencies (i.e. the vulnerability result will be likely equal to 1).

7. Discussion

The vulnerability of the IEEE 24 nodes reliability test system has been analysed. Different metrics have been compared in ranking contingencies and the

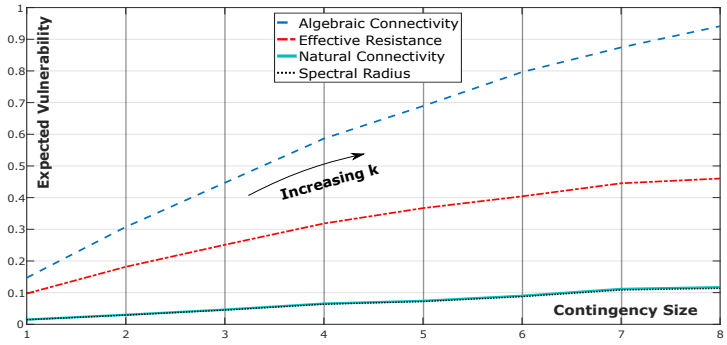

Figure 11: Comparison between the expected vulnerability when facing an $N-k$ contingencies using different spectral metrics. Adjacency built using B_{ij} as weights.

uncertainty due to load demands variability and line parameters imprecision has been quantified.

The comparison between pure topological and extended topological approaches shows significant correlation (similarities) between the ranking results. Spectral analysis of the network requires a moderate computational cost for obtaining a full spectrum of eigenvalues and eigenvectors for each contingency; significantly less than the cascading indices. The higher computational complexity is attributable to the (at least two) power flow solutions which have to be computed to obtain the cascading indices. Of course, the larger the network size the higher will be the computational cost for the analysis. Nevertheless, adjacency matrices for real world power network are often sparse matrix and, therefore, dedicated approaches can be used to speed up the procedure when just few eigenvalues are needed, e.g. spectral radius and algebraic connectivity. In this case, the on-line applicability of the spectral vulnerability metric for contingency ranking also accounting uncertainties might be feasible.

However, the spectral vulnerability metrics, even if enhanced by electrical engineering concepts, seem unable to fully capture the complexity of the network operation, i.e. major difference has been observed between cascading index results and results using extended topological approaches. Nevertheless, many of the lines which have been ranked using cascading indices resulted in a null contribution to the vulnerability (due to null post-failure overload severity). This might be regarded as a limitation of the CEI metric which has not been able to fully capture all the relevant consequences of certain line failures.

The uncertainty in vulnerability metrics, due to the load demands variability and lines parameters imprecision (tolerances) has been quantified. This provides a more robust identification of the critical components. The line ranking results under uncertainty differ from the deterministic results, although some of the most critical line contingencies have been similarly identified. Analysing the output P-boxes, it has been observed that the vulnerability computed using spectral vulnerability metrics and power flow as the weighting factor is greatly affected by the stochastic load profile. Also tolerance imprecision (epistemic uncertainty) has a non-negligible effect, although its contribution to the uncertainty seems less significant on spectral vulnerability metrics. Conversely, some of cascading indices show high sensitivity to parameters imprecision.

As expected, the uncertainty propagation using advanced uncertainty quantification techniques was very demanding, especially for the power-flow methods. This is a clear limitation of the advanced UQ approach which makes it difficult to apply to on-line analysis. Nevertheless, the method is powerful and versatile and can be effectively used to point out how much of the output uncertainty is reducible by further data collection (i.e. due to lack of information). This can be useful in may ways. For instance, a decision makers can use the method to to determine if a power grid is robust, if it is vulnerable, or if the available

information is not sufficient to provide a clear answer to questions relating to the network ability to withstand targeted or random contingencies.

To summarise, select good vulnerability metrics for the identification of relevant contingencies is not an easy task. Among the different metrics considered in this work, pure topological metrics present two relevant features: 1) less information is generally required (only the structure of the grid was needed); 2) uncertainty associated to operative variables (e.g. load demand) and imprecision associated with power grid parameters are not affecting the metrics. These may be regarded as positive features, nonetheless, it might be argued that the pure topological metrics (being less sensitive to variability) are less effective in capturing complex behaviours which are typical of varying operative states in power grids. Although a correlation analysis pointed out some similarity between topological metrics and the cascading indices, their capabilities for contingency ranking prospects are still questionable. Further comparisons between graph-theory methods and traditional approaches are necessary.

8. Conclusions

In this paper, a novel framework for assessing power grids vulnerability has been presented. The vulnerability assessment framework is embedded to advanced uncertainty quantification methods used to quantify the level of epistemic and aleatory uncertainty on the results. Single line and multiple line contingencies have been analysed and their vulnerability ranked with respect to topology-based metrics, flow-based metrics and accounting for model imprecision and stochastic loads. Four spectral vulnerability metrics have been computed using four different weighting factors (taken from literature and newly defined) and used to assess the robustness of a modified version of the IEEE 24 nodes RTS. Different effects of epistemic and aleatory uncertainty on network operational weaknesses (i.e. AC and DC overflow cascading models) and structural vulnerabilities have been discussed and relevant differences in the contingency ranking have been pointed out. Major differences in ranking results are attributable to the different vulnerability metrics rather than to different line weights. In case that only one vulnerability metric is selected, the choice of metric must be done with a high degree of care and done so whilst accounting for all the relevant sources of uncertainty which may generate misleading results.

Acknowledgement

The authors would like to acknowledge the gracious support of this work through the EPSRC and ESRC Centre for Doctoral Training on Quantification and Management of Risk & Uncertainty in Complex Systems & Environments Grant number (EP/L015927/1)

References

[1] E. Zio, Challenges in the vulnerability and risk analysis of critical infrastructures, Reliability Engineering & System Safety 152 (2016) 137 – 150. doi:http://dx.doi.org/10.1016/j.ress.2016.02.009.
URL http://www.sciencedirect.com/science/article/pii/S0951832016000508

[2] A. Fichera, M. Frasca, R. Volpe, Complex networks for the integration of distributed energy systems in urban areas, Applied Energy 193 (2017) 336 – 345. doi:https://doi.org/10.1016/j.apenergy.2017.02.065.
URL http://www.sciencedirect.com/science/article/pii/S0306261917301836

[3] R. Rocchetta, Y. Li, E. Zio, Risk assessment and risk-cost optimization of distributed power generation systems considering extreme weather conditions, Reliability Engineering & System Safety 136 (0) (2015) 47 – 61. doi:http://dx.doi.org/10.1016/j.ress.2014.11.013.
URL http://www.sciencedirect.com/science/article/pii/S0951832014002956

[4] G. A. Pagani, M. Aiello, From the grid to the smart grid, topologically, Physica A: Statistical Mechanics and its Applications (2015) –doi:http://dx.doi.org/10.1016/j.physa.2015.12.080.
URL http://www.sciencedirect.com/science/article/pii/S0378437115011085

[5] Y. Koç, M. Warnier, P. V. Mieghem, R. E. Kooij, F. M. Brazier, The impact of the topology on cascading failures in a power grid model, Physica A: Statistical Mechanics and its Applications 402 (2014) 169 – 179. doi:http://dx.doi.org/10.1016/j.physa.2014.01.056.
URL http://www.sciencedirect.com/science/article/pii/S0378437114000776

[6] F. Xiao, J. McCalley, Power system risk assessment and control in a multiobjective framework, Power Systems, IEEE Transactions on 24 (1) (2009) 78–85. doi:10.1109/TPWRS.2008.2004823.

[7] J. Bialek, E. Ciapessoni, D. Cirio, E. Cotilla-Sanchez, C. Dent, I. Dobson, P. Henneaux, P. Hines, J. Jardim, S. Miller, M. Panteli, M. Papic, A. Pitto, J. Quiros-Tortos, D. Wu, Benchmarking and validation of cascading failure analysis tools, IEEE Transactions on Power Systems 31 (6) (2016) 4887–4900. doi:10.1109/TPWRS.2016.2518660.

[8] Y. Koç, M. Warnier, P. V. Mieghem, R. E. Kooij, F. M. Brazier, A topological investigation of phase transitions of cascading failures in power grids, Physica A: Statistical Mechanics and its Applications 415 (2014) 273 – 284. doi:http://dx.doi.org/10.1016/j.physa.2014.07.083.

URL http://www.sciencedirect.com/science/article/pii/S0378437114006694

[9] G. J. Correa, J. M. Yusta, Grid vulnerability analysis based on scale-free graphs versus power flow models, Electric Power Systems Research 101 (2013) 71 – 79. doi:http://doi.org/10.1016/j.epsr.2013.04.003.
URL http://www.sciencedirect.com/science/article/pii/S0378779613000977

[10] E. Bompard, D. Wu, F. Xue, Structural vulnerability of power systems: A topological approach, Electric Power Systems Research 81 (7) (2011) 1334 – 1340. doi:http://dx.doi.org/10.1016/j.epsr.2011.01.021.
URL http://www.sciencedirect.com/science/article/pii/S0378779611000332

[11] S. Cvijic, M. Ilic, On limits to the graph-theoretic approaches in the electric power systems, in: 2011 North American Power Symposium, 2011, pp. 1–6. doi:10.1109/NAPS.2011.6025160.

[12] P. Hines, E. Cotilla-Sanchez, S. Blumsack, Do topological models provide good information about electricity infrastructure vulnerability?, Chaos: An Interdisciplinary Journal of Nonlinear Science 20 (3) (2010) 033122. arXiv:http://dx.doi.org/10.1063/1.3489887, doi:10.1063/1.3489887.
URL http://dx.doi.org/10.1063/1.3489887

[13] S. LaRocca, J. Johansson, H. Hassel, S. Guikema, Topological performance measures as surrogates for physical flow models for risk and vulnerability analysis for electric power systems, Risk Analysis 35 (4) (2015) 608–623. doi:10.1111/risa.12281.
URL http://dx.doi.org/10.1111/risa.12281

[14] R. Rocchetta, E. Patelli, Power grid robustness to severe failures: Topological and flow based metrics comparison, in: ECCOMAS Congress 2016 - Proceedings of the 7th European Congress on Computational Methods in Applied Sciences and Engineering, Vol. 3, 2016, pp. 6121–6135. doi:10.7712/100016.2246.10737.
URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-84995495513&doi=10.7712%2f100016.2246.10737&partnerID=40&md5=40727b123b64089527ee694df792a3f1

[15] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jimnez-Fernndez, Z. W. Geem, A critical review of robustness in power grids using complex networks concepts, Energies 8 (9) (2015) 9211. doi:10.3390/en8099211.
URL http://www.mdpi.com/1996-1073/8/9/9211

[16] M. A. Matos, E. Gouveia, The fuzzy power flow revisited, in: 2005 IEEE Russia Power Tech, 2005, pp. 1–7. doi:10.1109/PTC.2005.4524683.

[17] G. Sansavini, R. Piccinelli, L. Golea, E. Zio, A stochastic framework for uncertainty analysis in electric power transmission systems with wind generation, Renewable Energy 64 (2014) 71 – 81. doi:http://dx.doi.org/10.1016/j.renene.2013.11.002.
URL http://www.sciencedirect.com/science/article/pii/S0960148113005806

[18] G. J. Correa, J. M. Yusta, Structural vulnerability in transmission systems: Cases of Colombia and Spain, Energy Conversion and Management 77 (2014) 408 – 418. doi:https://doi.org/10.1016/j.enconman.2013.10.011.
URL http://www.sciencedirect.com/science/article/pii/S0196890413006316

[19] R. Mena, M. Hennebel, Y.-F. Li, C. Ruiz, E. Zio, A risk-based simulation and multi-objective optimization framework for the integration of distributed renewable generation and storage, Renewable and Sustainable Energy Reviews 37 (2014) 778 – 793. doi:http://dx.doi.org/10.1016/j.rser.2014.05.046.
URL http://www.sciencedirect.com/science/article/pii/S1364032114003712

[20] Y. Li, G. Sansavini, E. Zio, Non-dominated sorting binary differential evolution for the multi-objective optimization of cascading failures protection in complex networks, Reliability Engineering & System Safety 111 (2013) 195 – 205. doi:https://doi.org/10.1016/j.ress.2012.11.002.
URL http://www.sciencedirect.com/science/article/pii/S0951832012002311

[21] E. Ferrario, N. Pedroni, E. Zio, Evaluation of the robustness of critical infrastructures by hierarchical graph representation, clustering and monte carlo simulation, Reliability Engineering & System Safety 155 (2016) 78 – 96. doi:https://doi.org/10.1016/j.ress.2016.06.007.
URL http://www.sciencedirect.com/science/article/pii/S0951832016301120

[22] T. Ding, Y. Lin, Z. Bie, C. Chen, A resilient microgrid formation strategy for load restoration considering master-slave distributed generators and topology reconfiguration, Applied Energy 199 (2017) 205 – 216. doi:https://doi.org/10.1016/j.apenergy.2017.05.012.
URL http://www.sciencedirect.com/science/article/pii/S0306261917305056

[23] R. J. Snchez-Garca, M. Fennelly, S. Norris, N. Wright, G. Niblo, J. Brodzki, J. W. Bialek, Hierarchical spectral clustering of power grids, IEEE Transactions on Power Systems 29 (5) (2014) 2229–2237. doi:10.1109/TPWRS.2014.2306756.

[24] Y. P. Fang, E. Zio, Unsupervised spectral clustering for hierarchical modelling and criticality analysis of complex networks, Reliability Engineering & System Safety 116 (2013) 64 – 74. doi:https://doi.org/10.1016/j.ress.2013.02.021.
URL http://www.sciencedirect.com/science/article/pii/S0951832013000562

[25] Q. Chen, J. D. McCalley, Identifying high risk n-k contingencies for online security assessment, IEEE Transactions on Power Systems 20 (2) (2005) 823–834. doi:10.1109/TPWRS.2005.846065.

[26] E. van Dam, R. Kooij, The minimal spectral radius of graphs with a given diameter, Linear Algebra and its Applications 423 (2) (2007) 408 – 419. doi:http://dx.doi.org/10.1016/j.laa.2007.01.011.
URL http://www.sciencedirect.com/science/article/pii/S002437950700047X

[27] G. S. Peng, J. Wu, Optimal network topology for structural robustness based on natural connectivity, Physica A: Statistical Mechanics and its Applications 443 (2016) 212 – 220. doi:http://dx.doi.org/10.1016/j.physa.2015.09.023.
URL http://www.sciencedirect.com/science/article/pii/S0378437115007505

[28] E. Estrada, N. Hatano, M. Benzi, The physics of communicability in complex networks, Physics Reports 514 (3) (2012) 89 – 119, the Physics of Communicability in Complex Networks. doi:https://doi.org/10.1016/j.physrep.2012.01.006.
URL http://www.sciencedirect.com/science/article/pii/S0370157312000154

[29] E. Patelli, D. Alvarez, M. Broggi, M. De Angelis, Uncertainty management in multidisciplinary design of critical safety systems, Journal of Aerospace Information Systems 12 (1) (2015) 140–169, cited By 3. doi:10.2514/1.I010273.
URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-84922432517&doi=10.2514%2f1.I010273&partnerID=40&md5=692dfe1597398e379caaad3735476d61

[30] A. Rosengart, M. Vizzi, F. Manenti, A. Citterio, Development of an ultrafiltration predictive model to estimate the cost of downstream in biorefineries: Effects of epistemic experimental uncertainties, Energy Conversion and Management (2017) – doi:https://doi.org/10.1016/j.enconman.2017.03.043.
URL http://www.sciencedirect.com/science/article/pii/S0196890417302546

[31] A. P. Dempster, A generalization of bayesian inference, Journal of the Royal Statistical Society. Series B (Methodological) 30 (2) (1968) 205–247.
URL http://www.jstor.org/stable/2984504

[32] M. Beer, S. Ferson, V. Kreinovich, Imprecise probabilities in engineering analyses, Mechanical Systems and Signal Processing 37 (12) (2013) 4 – 29. doi:http://dx.doi.org/10.1016/j.ymssp.2013.01.024.
URL http://www.sciencedirect.com/science/article/pii/S0888327013000812

[33] H. A. Jensen, Structural optimal design of systems with imprecise properties: a possibilistic approach, Advances in Engineering Software 32 (12) (2001) 937 – 948. doi:http://dx.doi.org/10.1016/S0965-9978(01)00038-2.
URL http://www.sciencedirect.com/science/article/pii/S0965997801000382

[34] S. Destercke, D. Dubois, E. Chojnacki, Unifying practical uncertainty representations i: Generalized p-boxes, International Journal of Approximate Reasoning 49 (3) (2008) 649 – 663.
URL http://www.sciencedirect.com/science/article/pii/S0888613X0800114X

[35] G. Shafer, A Mathematical Theory of Evidence, Princeton University Press, Princeton, 1976.

[36] P. Edoardo, COSSAN: A Multidisciplinary Software Suite for Uncertainty Quantification and Risk Management, Springer International Publishing, Cham, 2016, pp. 1–69. doi:10.1007/978-3-319-11259-6_59-1.

[37] R. Rocchetta, E. Patelli, Imprecise probabilistic framework for power grids risk assessment and sensitivity analysis, in: Risk, Reliability and Safety: Innovating Theory and Practice, 2016, pp. 2789–2796. doi:10.1201/9781315374987-424.

[38] Z. Qiu, Y. Xia, J. Yang, The static displacement and the stress analysis of structures with bounded uncertainties using the vertex solution theorem, Computer Methods in Applied Mechanics and Engineering 196 (49-52) (2007) 4965–4984, cited By 56. doi:10.1016/j.cma.2007.06.022.
URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-34548727350&doi=10.1016%2fj.cma.2007.06.022&partnerID=40&md5=cfd2c6905fb35a987ddf6a2bf1dd0254

[39] E. Ciapessoni, D. Cirio, G. Kjlle, S. Massucco, A. Pitto, M. Sforna, Probabilistic risk-based security assessment of power systems considering incumbent threats and uncertainties, IEEE Transactions on Smart Grid 7 (6) (2016) 2890–2903. doi:10.1109/TSG.2016.2519239.

[40] R. D. Zimmerman, C. E. Murillo-Sanchez, R. J. Thomas, Matpower: Steady-state operations, planning, and analysis tools for power systems research and education, IEEE Transactions on Power Systems 26 (1) (2011) 12–19. doi:10.1109/TPWRS.2010.2051168.

[41] P. Wong, P. Albrecht, R. Allan, R. Billinton, Q. Chen, C. Fong, S. Haddad, W. Li, R. Mukerji, D. Patton, A. Schneider, M. Shahidehpour, C. Singh, The ieee reliability test system-1996. a report prepared by the reliability test system task force of the application of probability methods subcommittee, Power Systems, IEEE Transactions on 14 (3) (1999) 1010–1020. doi:10.1109/59.780914.

[42] D. Van Hertem, J. Verboomen, K. Purchala, R. Belmans, W. Kling, Usefulness of dc power flow for active power flow analysis with flow controlling devices, in: AC and DC Power Transmission, 2006. ACDC 2006. The 8th IEE International Conference on, 2006, pp. 58–62.

[43] W. Pirie, Spearman Rank Correlation Coefficient, John Wiley & Sons, Inc., 2004. doi:10.1002/0471667196.ess2499.pub2.
URL http://dx.doi.org/10.1002/0471667196.ess2499.pub2